Dell EMC Integrated Data Protection Appliance

Versión 2.2

Guía del producto

302-004-956

REV. 01

DELL EMC

Publicado en Junio de 2018

Dirección local de EMC
EMC Argentina (Cono Sur) Tel. +54-11-4021-3622 http://www.emc.com/es-ar/index.htm
EMC México Tel. +52-55-5080-3700 http://www.emc.com/es-mx/index.htm
EMC Venezuela (Norte de Latinoamérica) Tel. +58-212-206-6911 http://www.emc.com/es-ve/index.htm

CONTENIDO

Historial de revisiones

Tabla 1 Historial de revisiones de la Guía del producto IDPA 2.2

Revisión	Fecha	Descripción
01	Junio de 2018	Versión 2.2

CAPÍTULO 1

Introducción

En este capítulo, se proporciona una descripción general de las características y configuraciones de hardware de Integrated Data Protection Appliance 2.2.

Se abordarán los siguientes temas:

Alcance del documento y público objetivo

El alcance de este documento es describir los detalles administrativos de Integrated Data Protection Appliance (IDPA).

El público objetivo de este documento incluye personal de campo, partners y clientes responsables de la administración y la operación de IDPA. Este documento se creó para personas que están familiarizadas con las soluciones de Dell EMC Protección de datos.

Características del producto

IDPA proporciona una configuración simplificada y la integración de componentes de protección de datos en una solución consolidada.

Implementación y configuración simplificadas
IDPA modelo DP4400 es un sistema de 2U hiperconvergente que un usuario puede instalar y configurar en el sitio.

El software del sistema para cada componente se instala y se configura en la mayor medida posible antes de enviar el dispositivo. El dispositivo trae incorporado lo siguiente: aplicación de respaldo, almacenamiento de destino, creación de informes y analítica, búsqueda y Appliance Configuration Manager (ACM).

Esta versión incluye el IDPA System Manager y agrega la recuperación ante desastres en la nube (CDRA) opcional a la pila de software.

Administración centralizada
ACM proporciona una interfaz gráfica basada en Web para configurar, monitorear y actualizar el dispositivo. IDPA System Manager proporciona funcionalidades avanzadas de administración y monitoreo de IDPA desde un solo panel e incluye las siguientes características:

- Tableros integrales que incluyen la siguiente información del sistema de Avamar y IDPA:
  - Actividades de respaldo
  - Actividades de replicación
  - Capacidad
  - Estado
  - Alertas
- El monitoreo de múltiples funcionalidades incluye el estado del sistema y las actividades.
- Funcionalidades de administración para la aplicación de respaldo.
- Operaciones avanzadas de búsqueda y recuperación mediante la integración con Search.
- Funcionalidades de creación de informes.

Administración de respaldo
IDPA protege los clientes virtuales y físicos, los distintos tipos de sistemas de archivos, las aplicaciones y las bases de datos

Monitoreo y analítica
La función de monitoreo y analítica ofrece una sólida funcionalidad de creación de informes con secciones específicas para diversas funciones. Los informes lo ayudan a

recuperar información acerca del ambiente para que pueda revisar y analizar las actividades en el ambiente. Con estos informes, puede identificar interrupciones en el ambiente, diagnosticar problemas, planificar tareas para disminuir los riesgos y pronosticar tendencias futuras. Según los requisitos empresariales, puede ejecutar plantillas personalizadas de informes y de tableros según demanda o programadas en intervalos definidos.

El tablero de ACM muestra un resumen de la configuración de los componentes individuales y permite al administrador monitorear el dispositivo, cambiar los detalles de configuración o actualizar el sistema y sus componentes. El tablero también muestra información sobre las alertas de estado del dispositivo para el servidor y los componentes de VMware.

Search
La función Search proporciona una manera eficaz para buscar datos de respaldo dentro de IDPA y, a continuación, restaurar el respaldo o descargar los resultados de búsqueda. Las actividades de recopilación programadas se usan para recopilar e indexar los metadatos, que luego se almacenan dentro de IDPA.

Recuperación ante desastres
DD Cloud DR es una solución opcional que facilita la recuperación de máquinas virtuales en las instalaciones, ya que proporciona la capacidad de recuperar esas máquinas virtuales en la nube. DD Cloud DR se integra con la aplicación de respaldo dentro de IDPA para copiar los respaldos de datos de máquinas virtuales a la nube pública. A continuación, puede realizar pruebas de DR o conmutación por error de los ambientes de producción mediante la organización de una conversión completa de la máquina virtual a una instancia de Elastic Compute Cloud (EC2) de Amazon Web Services y mediante la ejecución de esta instancia en la nube.

CDRA es una aplicación incorporada que administra la implementación de la infraestructura necesaria para la nube y la copia de los respaldos de máquinas virtuales a la nube, y organiza la compresión, el cifrado y la copia de los datos respaldados de VM a la nube.

Nota

CDRA es opcional.

Escalabilidad
IDPA está diseñado para ser escalable, de modo que puede crecer con las necesidades cambiantes. La configuración básica de DP4400 incluye 24 TB de espacio de almacenamiento, que se puede expandir con licencia de capacidad adicional en incrementos de 12 TB hasta un máximo de 96 TB.

Soporte unificado
El mismo equipo de Servicio al cliente es compatible con el hardware y el software utilizados en el dispositivo.

Nota

IDPA es compatible con redes activadas para IPv4 y no se admite en un ambiente IPv6 puro o en redes de doble pila.

Arquitectura y componentes del sistema

IDPA combina múltiples soluciones de protección de datos en un solo producto.

Configuración detallada

IDPA está disponible en los siguientes modelos:

Tabla 2 Opciones de configuración para cada modelo

Modelo	Modelo de almacenamiento con protección	Opciones de configuración de almacenamiento con protección (TB utilizables)	Servidor de respaldo	Nodo acelerador de Avamar para respaldo de NDMP/NAS (opcional)
DP4400	Data Domain Virtual Edition	24, 36, 48, 60, 72, 84 o 96 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1)
DP5300	Data Domain 6300	34, 82 o 130 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1)
DP5800	Data Domain 6800	144, 96, 192, 240 o 288 TB	Avamar Virtual Edition 3 TB	NDMP Accelerator (1-3)
DP8300	Data Domain 9300	192, 240, 288, 336, 384, 432, 480, 528, 576, 624, 672 o 720 TB	Cuadrícula de Avamar: • Un nodo de utilidad • Tres nodos de almacenamiento M1200 (12 TB) • Dos switches	NDMP Accelerator (1-4)
DP8800	Data Domain 9800	624, 672, 720 768, 816, 864, 912, 960 o 1,008 TB	Cuadrícula de Avamar: • Un nodo de utilidad • Cuatro nodos de almacenamiento M1200 (16 TB) • Dos switches	NDMP Accelerator (1-4)

Software integrado

Después de la configuración inicial, se implementa y se configura el siguiente software:

- Data Domain Virtual Edition (DDVE)
- Máquina virtual de VMware vCenter Server (plataforma de la arquitectura interna en la que se ejecuta el dispositivo)
- VMware ESXi
- Avamar Virtual Edition (AVE)
- Máquina virtual del proxy de Avamar
- Integrated Data Protection Appliance System Manager VM
- Data Protection Advisor
  - Máquina virtual del host de Application Server
  - Máquina virtual host de Datastore Server
- Data Protection Search

    - Máquina virtual del host del nodo de índice maestro
- Dispositivo virtual DD Cloud DRCDRA (opcional)
- Appliance Configuration Manager

Protección automática del sistema

IDPA está configurado para protegerse contra la pérdida de datos con las aplicaciones de almacenamiento y respaldo incluidas en el sistema. El sistema está protegido con trabajos de respaldo definidos e iniciados automáticamente, que se programan a diario y tienen un período de retención de 30 días. Los metadatos del sistema se protegen mediante respaldo de punto de control para el almacenamiento de destino interno.

Descripción general de la conectividad de red

Cuando se utiliza un rango de direcciones IP durante la configuración de IDPA, se asignan las direcciones IP en un orden estándar. Utilice la tabla a continuación para determinar qué dirección IP se asigna a un componente.

La primera columna de cada tabla, Asignación de rango de IP, es el valor que se debe agregar a la primera dirección IP en el rango.

Tabla 3 Asignaciones de rango de direcciones IP para DP4400

Asignación de rango de IP	Ejemplo	Componente	Campo asignado
+0	`192.0.2.1`	vCenter	Máquina virtual de VMware vCenter Server
+1	`192.0.2.2`	Almacenamiento de destino	IP de datos 1
+2	`192.0.2.3`	Almacenamiento de destino	IP de datos 2
+3	`192.0.2.4`	Almacenamiento de destino	IP de datos 3
+4	`192.0.2.5`	Aplicación de respaldo	IP del servidor
+5	`192.0.2.6`	Aplicación de respaldo	VM de proxy Avamar
+6	`192.0.2.7`	IDPA System Manager	VM de IDPA System Manager
+7	`192.0.2.8`	Analítica y creación de informes	Máquina virtual del host del servidor de aplicaciones
+8	`192.0.2.9`	Analítica y creación de informes	Máquina virtual del host del servidor de almacenamiento de datos
+9	`192.0.2.10`	Search	Máquina virtual del host del nodo de índice maestro
+10	`192.0.2.11`	DD Cloud DRCDRA (opcional)	Dispositivo virtual Data Domain Cloud Disaster Recovery (DD Cloud DR) Complemento de Cloud DR (CDRA)

CAPÍTULO 2

Monitoreo y administración del dispositivo

En este capítulo, se presentan las características y funcionalidades del tablero ACM.

Se abordarán los siguientes temas:

Acerca del tablero

El tablero de ACM le permite administrar la configuración para el dispositivo y los componentes individuales, actualizar información de soporte del cliente y actualizar el software para el dispositivo y sus componentes.

Para acceder al tablero, escriba `https://<ACM IP address>:8543/` en un navegador web e inicie sesión. El tablero requiere Google Chrome 64.0.3282.140 o versiones posteriores, o Mozilla Firefox 47.2 o versiones posteriores.

Nota

El tablero se activa solamente después de configurar IDPA.

En la vista inicial, se visualiza la página **Home** y las pestañas **Health** y **Upgrade**.

Tareas de administración básicas

Vea los detalles del sistema, cambie la contraseña de los componentes del dispositivo y cierre la sesión en el tablero.

Cambio de la contraseña de ACM

1. Haga clic en el icono **Change Password**.
2. Escriba la contraseña actual en **Current Password**.
3. Escriba la nueva contraseña en **New Password** y confírmela.
4. Haga clic en **Change Password**.

Nota

La contraseña debe tener entre 9 y 20 caracteres, y debe incluir al menos un carácter compatible de cada tipo. Los siguientes tipos de caracteres son compatibles:

- Letras en mayúscula (`A-Z`)
- Letras en minúscula (`a-z`)
- Números (`0-9`)
- Caracteres especiales: punto (`.`), guion (`-`) y guion bajo (`_`)

La contraseña no debe incluir nombres comunes o nombres de usuario como `root` o `admin`.

El usuario cambia la contraseña en la siguiente secuencia:

1. Usuario de LDAP interno de ACM `idpauser`.
2. Usuario de almacenamiento (DDVE) `sysadmin`.
3. Usuarios del servidor de respaldo (Avamar):
   a. `Admin` y `root` del SO.
   b. Usuarios del servidor Avamar: `root`, `mcuser`, `repulser` y `viewuser`.
4. Usuario `root` del SO del proxy del servidor de respaldo.
5. Usuarios de IDPA System Manager (DPC): `Admin` y `root` del SO.
6. Usuarios de Reporting and Analytics (DPA): `Root` de SO de Application Server, `root` de SO de Datastore, y `administrator`de Application Server.

7. `Root` de SO de búsqueda (DPS) y `root` y `admin` de LDAP predeterminado de búsqueda.
8. Contraseña de `admin` de Cloud Disaster Recovery (CDRA).
9. Contraseña de `idpauser` de VCenter y ESXi.
10. Contraseña de root de ACM.

Nota

Después de cambiar la contraseña, los usuarios de ACM deben cerrar la sesión e iniciar sesión nuevamente con la contraseña actualizada.

Visualización de detalles de versión y compilación
Haga clic en el icono **Information** (**i**). En la página **About** se muestran los detalles sobre el número de versión y compilación de IDPA.

Cerrar sesión
Haga clic en el botón **Log Out**.

Pestaña Home del tablero ACM

La pestaña **Home** proporciona una descripción general del estado y la configuración para IDPA y cada componente.

En la pestaña **Home** del tablero, puede ver los detalles del producto y la configuración de red; administrar la contraseña, la zona horaria y la configuración de NTP, SNMP y SMTP; y modificar la información de soporte del cliente.

También puede configurar LDAP, crear y descargar paquetes de registros, actualizar la contraseña común en todos los componentes, registrar componentes con Secure Remote Services (anteriormente conocido como ESRS) e instalar los componentes opcionales (CDRA).

Nota

El vínculo de configuración de Secure Remote Services está presente en el menú del icono de engranaje. Mueva el cursor del mouse sobre el icono de engranaje para ver la lista de todas las opciones de menú.

Si falla DPS o DPA durante la configuración, ACM no detiene toda la configuración. El proceso de configuración sigue funcionando hasta completarse. Cuando finaliza el proceso de configuración, el tablero de ACM proporciona una opción para configurar el componente fallido (DPS o DPA).

Descarga de los detalles de configuración
Para descargar un archivo PDF con los detalles actuales de la configuración de IDPA, haga clic en el icono de Adobe PDF.

Administración de los componentes del sistema
La pestaña **Home** contiene los paneles para cada una de las siguientes funciones:

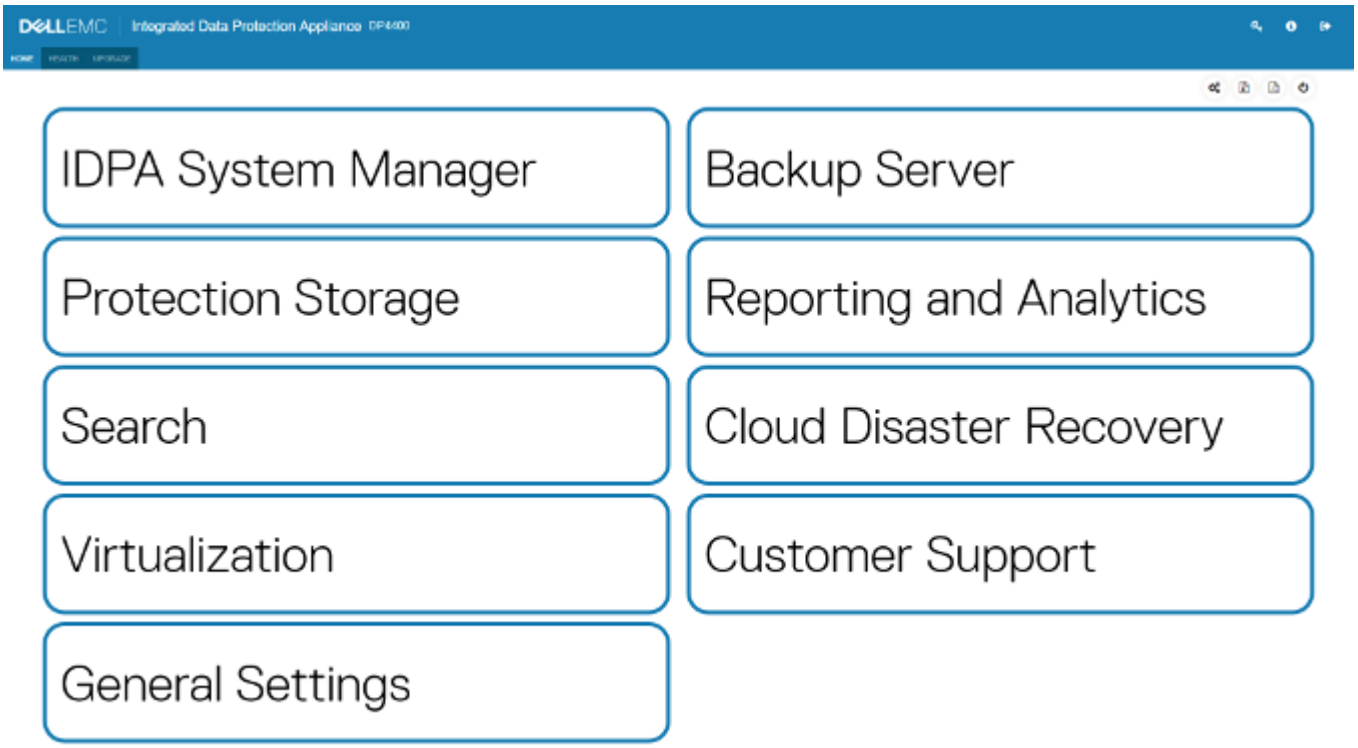
- **IDPA System Manager**
- **Backup Server**
- **Protection Storage**
- **Reporting and Analytics**
- **Search**
- **Cloud Disaster Recovery**

- **Virtualization**
- **Servicio al cliente**
- **General Settings**

Nota

Si hay un componente al que no se puede acceder en la red o que tiene una credencial almacenada incorrecta, el panel correspondiente le indica al usuario que resuelva el problema.

Figura 1 Diseño del inicio del tablero de ACM sin los detalles individuales del panel



Nota

Cuando ACM se reinicia, intenta iniciar cada componente. Esto puede afectar la velocidad de funcionamiento de la interfaz del usuario de ACM.

Panel IDPA System Manager

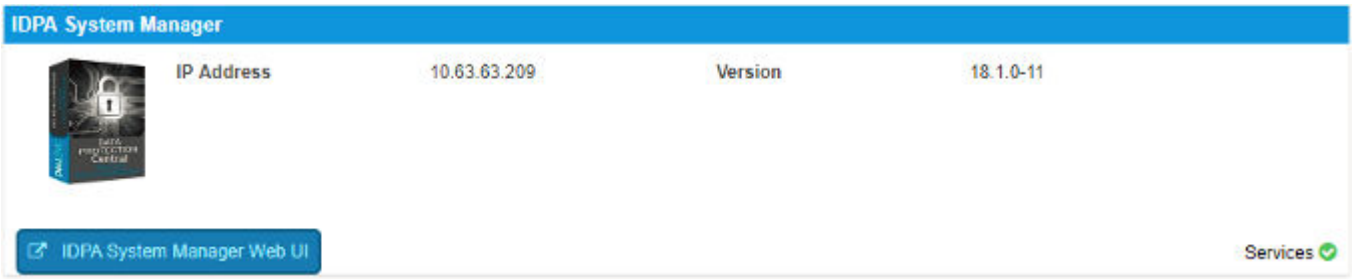
En el panel **IDPA System Manager**, se muestra la versión de IDPA System Manager y la dirección IP del componente. Para iniciar **IDPA System Manager Web UI**, haga clic en el botón e inicie sesión.

Nota

Si no se configuró LDAP externo, utilice `idpauser` como nombre de usuario. Si se configuró LDAP externo, utilice el nombre de usuario de LDAP.

Mueva el cursor a **Services** para ver información de estado de los servicios de IDPA System Manager.

Figura 2 Panel **IDPA System Manager** en la página **Home** de ACM



Para obtener más información sobre los flujos de trabajo y las funcionalidades de IDPA System Manager, consulte la *IDPA System Manager Guía de administración*.

Panel Backup Server

En el panel **Backup Server**, se muestra la dirección IP del componente, la versión de Avamar, el almacenamiento de metadatos de respaldo total y disponible, el estado de la licencia del nodo del servidor de respaldo y si la instalación de agentes está en curso. Haga clic en el vínculo **Download Agents** que aparece después de que finaliza la instalación del agente para cargar la GUI de restauración web de Avamar, desde la que se pueden cargar los agentes de Avamar.

Figura 3 Panel **Backup Server** en la página **Home** de ACM

Para obtener más información acerca de la función de los agentes de respaldo y cómo instalarlos, consulte la *Avamar Guía de administración*. Mueva el cursor a **Services** para ver información de estado de los servicios de Avamar.

Habilitación de verificación del certificado

De forma predeterminada, la comprobación de certificados de vCenter está deshabilitada en IDPA.

IDPA utiliza una versión modificada del archivo Avamar`MCServer.xml`. Durante la configuración, esta modificación hace que los certificados de vCenter se ignoren cuando se agregan vCenter Servers. Para habilitar la comprobación de certificado:

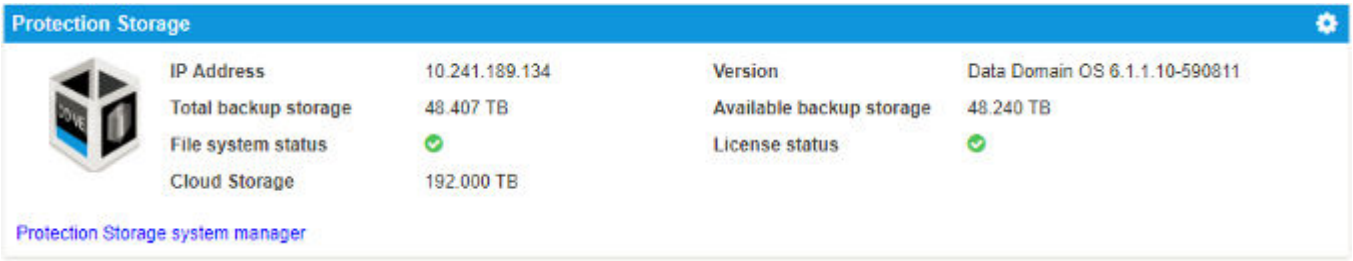
1. Cambie el valor `ignore_vc_cert` en el archivo a `false`.
2. Reinicie el servicio de MC con `dpnctl`.
3. Detenga `mcs` y `dpctl`.
4. Inicie los comandos `mcs` en el servidor Avamar.

Panel Protection Storage

En el panel **Protection Storage**, se visualiza la versión de DD OS, la dirección IP del componente, el almacenamiento de respaldo total y disponible, el sistema de archivos y el estado de licencia del nodo de almacenamiento con protección, y todas las alertas

que requieren acción por parte del usuario. Para acceder a una funcionalidad adicional del componente, haga clic en el vínculo **Protection Storage System Manager**.

Figura 4 Panel **Protection Storage** en la página **Home** de ACM



Expansión de la capacidad de almacenamiento

Puede agregar almacenamiento para Data Domain a fin de expandir la capacidad del nodo de almacenamiento con protección. El incremento del almacenamiento adjunto requiere licencias adicionales.

Antes de comenzar

- Obtenga licencias para la mayor capacidad de almacenamiento.

Una vez que el sistema detecta el hardware, la opción **Expand storage** está disponible en el menú del icono de engranaje.

Procedimiento

1. En el panel **Protection Storage**, active con el mouse el icono de engranaje en la parte superior derecha y haga clic en **Expand storage**.

   Se abre el asistente **Storage expansion and license upgrade**.
2. Haga clic en **Browse** y seleccione los archivos de licencia requeridos para el almacenamiento adicional.
3. Haga clic en **Expand**.

Resultados

Después de varios minutos, el tablero refleja la mayor capacidad de almacenamiento.

Configuración de la función de retención a largo plazo de la nube en IDPA.

DD Cloud Tier se establece a través de la configuración de ACM. Siga los procedimientos a continuación para crear unidades de nube de DD y configure las políticas de respaldo de Avamar para LTR en la nube.

Antes de comenzar

Nota

Para obtener información detallada sobre la creación de unidades de nube de DD, consulte *Data Domain Operating System: guía de administración*.

Este proceso se refiere a los procedimientos descritos en los siguientes documentos:

- *Data Domain Operating System: guía de administración* para DD OS 6.0 o superior
- *Avamar y Guía de integración de sistemas Data Domain* para Avamar 7.4 o superior

Procedimiento

1. En la pestaña de inicio de **ACM**, haga clic en el vínculo **Protection Storage System Manager**.

   Se muestra la GUI **Data Domain System Manager**.

2. Siga el procedimiento "Importación de certificados de CA" que se describe en la *Data Domain Operating System: guía de administración*.

   Después de importar el certificado, cierre **Data Domain System Manager**.

3. Conéctese a la interfaz del usuario de Avamar mediante IDPA System Manager.

   Se muestra la GUI **Avamar Administrator**.

4. Siga el procedimiento "Adición o edición de un sistema Data Domain con soporte de organización de la nube en niveles" que se describe en la *Avamar y Guía de integración de sistemas Data Domain*.

   Nota

   ACM hace que el paso que se refiere a "Adición de un sistema Data Domain" sea innecesario. Para obtener información sobre cómo acceder al cuadro de diálogo **Edit Data Domain System**, consulte "Edición de un sistema Data Domain".

5. Siga el procedimiento "Crear un nuevo grupo de nivel" que se describe en la *Avamar y Guía de integración de sistemas Data Domain*.
6. Para verificar su configuración, haga clic en el botón de inicio **Activity** en **Avamar Administrator** y revise la lista de sesiones en la pestaña **Activity Monitor**.

Panel Reporting and Analytics

En el panel **Reporting and Analytics**, se muestran la versión de DP Advisor, las direcciones IP de Application Server y Datastore Server, el estado de la licencia del nodo de informes y análisis, y cualquier alerta que requiera una acción por parte del usuario. Para cargar la consola Reporting and Analytics, haga clic en el vínculo **Reporting and Analytics Web UI**. Mueva el cursor a **Services** para ver información de estado de los servicios de DP Advisor.

Figura 5 Panel **Reporting and Analytics** en la página **Home** de ACM

Si DP Advisor no se configuró durante el proceso de configuración inicial, en el panel se muestra un mensaje que indica que la opción Reporting and Analytics no está configurada. Para configurar el nodo de informes y análisis, haga clic en el mensaje. Aparece la pantalla Reporting and Analytics Configuration. En la pantalla **Reporting and Analytics Configuration**, proporcione las direcciones IP y la información de licencia requerida y, a continuación, haga clic en **Configure**.

Panel Search

En el panel **Search**, se muestra la versión de Search, para el nodo de índice maestro y cualquier alerta que requiera la acción por parte del usuario. Para cargar la consola Search, haga clic en el vínculo **Search**. Mueva el cursor a **Services** para ver información de estado de los servicios de Search.

Figura 6 Panel **Search** en la página **Home** de ACM

Si Search no se configuró durante el proceso de configuración inicial, el panel muestra un mensaje que indica que la búsqueda no está configurada. Para configurar el nodo de búsqueda, haga clic en el mensaje. Aparece la pantalla Search Configuration. En la pantalla **Search Configuration**, proporcione la dirección IP requerida y haga clic en **Configure**.

Configuración de clientes en Search

Todos los dominios en Avamar se indexan automáticamente. Solo deberán agregarse manualmente los dominios de cliente que se agreguen tras la implementación de DPSearch.

Panel Cloud Disaster Recovery

El panel **Cloud Disaster Recovery** muestra la versión de CDRA y todas las alertas que requieren acción por parte del usuario. Para cargar la consola Cloud Disaster Recovery, haga clic en el vínculo **Cloud Disaster Recovery Web UI**.

Figura 7 Panel **Cloud Disaster Recovery** en la página **Home** de ACM.

Si CDRA no se configuró durante el proceso de configuración inicial, el panel muestra **Click here to configure Cloud Disaster Recovery**, lo cual indica que la recuperación ante desastres en la nube no está configurada. Para configurar el nodo de recuperación ante desastres en la nube, haga clic en el mensaje. Aparece la pantalla Cloud Disaster Recovery Configuration. En la pantalla **Cloud Disaster Recovery Configuration**, escriba la dirección IP y haga clic en **Configure**.

Nota

- No cambie la contraseña de usuario raíz de Avamar antes de configurar CDRA desde el tablero.
- No cambie la contraseña de usuario de DD Boost antes de configurar CDRA desde el tablero.
- Si la dirección de correo electrónico y la cuenta en la nube no están configuradas en CDRA, la página de inicio de sesión de CDRA no funciona. El usuario debe configurar manualmente la dirección de correo electrónico y la cuenta en la nube en CDRA.

Conexión a la cuenta de la nube e incorporación de destinos de Cloud DR

Conecte el CDRA a la cuenta de Amazon Web Services y agregue destinos a la cuenta.

Antes de comenzar

- Ha iniciado sesión en CDRA como administrador.
- Tiene una cuenta de AWS que ya está configurada antes de conectarse a la cuenta de la nube.

Nota

IDPA realiza la configuración de CDRA de forma automática.

Procedimiento

1. Haga clic en **Cloud Account** en la barra de menú.

   Se abre la página **Connect to Cloud Account**.
2. Haga clic en **Add Cloud Account**.
3. En el cuadro de diálogo **Connecting toAWS Cloud account**, introduzca la clave de acceso y la clave secreta para la cuenta de AWS. En http://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_access-keys.html se proporciona información sobre cómo obtener las claves de acceso y las claves secretas.
4. Para copiar la política de administración de identidades y de acceso (IAM), haga clic en **Copy IAM Policy**.

   Esta acción copia en el búfer una versión JSON de los permisos mínimos de cuenta de usuario de AWS que se requieren para la implementación de Cloud DR, que luego se pueden aplicar a AWS para establecer la política de permisos para el usuario de AWS.
5. Para ver la política de administración de identidades y de acceso (IAM) que representa los permisos mínimos de cuenta de usuario de AWS que se requieren para la implementación de recuperación de Cloud DR, haga clic en **Show IAM Policy**.
6. Para guardar la cuenta de la nube de AWS, haga clic en **Verify & Save**.

   CDRA verifica la existencia de la cuenta antes de guardar la información de la cuenta de la nube y cerrar el cuadro de diálogo **Connecting to AWS Cloud account**.

Nota

Cuando haya proporcionado credenciales para una cuenta de AWS, no podrá cambiar a otra cuenta de AWS.

Cómo agregar destinos de nube

Puede agregar uno o más destinos a la cuenta de nube que incluye la selección de un depósito de Amazon S3 y un método de cifrado.

Procedimiento

1. Haga clic en **Cloud Account** en la barra de menú.

   Se abre la página **Connect to Cloud Account**.

2. Haga clic en **Add Cloud DR Target** para configurar uno o más destinos de Cloud DR.

   El destino de Cloud DR es el depósito de S3 en AWS donde se escriben los datos cuando se respaldan las máquinas virtuales en la nube. El servidor de Cloud DR se implementa en uno de los destinos.

   Se abre el cuadro de diálogo **Add Cloud DR Target**.

3. Escriba un nombre para el destino Cloud DR.

   El nombre introducido aquí aparece en Avamar Administrator al crear una política de respaldo de Cloud DR.

4. Seleccione un depósito de Amazon S3 para el destino Cloud DR.

5. Haga clic en **Advance security option** y seleccione un método de cifrado:

Opción	Descripción
SSE-S3	Cifrado predeterminado (sin costo)
SSE-KMS	Cifrado de servicio de administración de claves (incurre en un costo)

Nota

Si selecciona el método de cifrado SSE-KMS, solo se admite la clave predeterminada administrada por el cliente. El cambio de la clave de cifrado podría causar errores con los archivos en el depósito de Amazon S3.

Para obtener más información sobre estos métodos de cifrado, consulte:

- SSE-S3 - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingServerSideEncryption.html
- SSE-KMS - https://docs.aws.amazon.com/AmazonS3/latest/dev/UsingKMSEncryption.html

6. Haga clic en **Add**.

Implementación del servidor de Cloud DR

Implemente CDRS en un destino específico de Cloud DR.

Antes de comenzar

- Los destinos de Cloud DR son obligatorios en la cuenta de AWS antes de realizar esta tarea. Conexión a la cuenta de la nube e incorporación de destinos de Cloud DR en la página 21 contiene información sobre cómo agregar destinos de Cloud DR a la cuenta de AWS.
- Se deben aceptar los términos de AWS Marketplace antes de implementar el servidor de Cloud DR.

Procedimiento

1. En la barra de menú, haga clic en el servidor de Cloud DR.
   - Si no hay ningún CDRS implementado, se abre la página **Deploy Cloud DR Server**.
   - Si hay CDRS implementados, se abre la página **Cloud DR Server**. No se pueden implementar instancias de CDR adicionales.
2. En la sección **Cloud DR Server Configuration**, seleccione el destino de Cloud DR en el que desee implementar **Cloud DR Server**.
3. Para asignar direcciones IP para la solución Cloud DR, proporcione **IPV4 CIDR Range**.
4. En la sección **User Configuration**, introduzca y confirme las contraseñas para los usuarios de CDRS Admin y CDRS Monitor.

   Las contraseñas deben:

   - Tener al menos ocho caracteres de longitud.
   - Incluir caracteres de al menos tres de los siguientes tipos:
     - Mayúscula: A-Z
     - Minúscula: a-z
     - Carácter numérico: 0-9
     - Caracteres especiales (no alfanuméricos)

   a. Introduzca y confirme las contraseñas para los usuarios de CDRS Admin y CDRS Monitor.

   b. Introduzca una dirección de correo electrónico para las solicitudes de restablecimiento de contraseña de DD Cloud DR.

      Cuando se instala correctamente el servidor de Cloud DR, AWS envía un correo electrónico a esta dirección para la verificación. Siga las instrucciones que aparecen en el correo electrónico en un plazo de 24 horas desde la implementación.
5. Para confirmar que acepta los términos de Marketplace, haga clic en la casilla de verificación **I have accepted the AWS Marketplace terms**.
6. Haga clic en **Deploy** Cloud DR Server.

   CDRA comienza la implementación de CDRS en el destino de Cloud DR. Si se produce un error durante la implementación, haga clic en **Cleanup** para eliminar los recursos de nube que crea CDRS y, a continuación, vuelva a intentar la implementación.

   La implementación de CDRS puede tardar hasta 30 minutos.

Si la implementación se realiza correctamente, aparece la página Cloud DR Server, que enumera el hostname del host de CDRS y la región. También se implementa lo siguiente:

- Una nube privada virtual (VPC).
- Un catálogo de servicios de base de datos relacionales (RDS) de Amazon, a fin de mantener los datos persistentes.
- Una subred privada para la comunicación entre RDS y CDRS.
- Una subred pública (modo estándar) o una subred privada (modo profesional) con acceso a Internet para utilizar mediante CDRS.
- La instancia EC2 de CDRS.

La instancia M4.Large se utiliza para la instancia de CDRS. Para reducir los costos de implementación, es posible que desee adquirir instancias reservadas de AWS; de lo contrario, se utiliza una instancia por demanda. Una dirección IP elástica se asigna automáticamente a la instancia de CDRS. No puede cambiar esta dirección IP.

Nota

Varios dispositivos de complemento de Cloud DR pueden conectarse a una sola instancia del servidor de Cloud DR. Sin embargo, un dispositivo de complemento de Cloud DR no se puede conectar a múltiples instancias del servidor de Cloud DR.

Resultados

Cuando se implemente CDRS, conéctese al servidor de Cloud DR; para ello, haga un clic en el hostname de CDRS.

Creación de imágenes de recuperación rápida para máquinas virtuales protegidas

Puede acelerar el proceso de recuperación con anticipación mediante la creación de imágenes de recuperación rápida para máquinas virtuales protegidas.

La creación de una imagen de recuperación rápida inicia el proceso de rehidratación y convierte los archivos VMDK en una imagen de máquina de Amazon (AMI). A continuación, el proceso de recuperación inicia la instancia recuperada desde la AMI.

Realice este procedimiento cuando haya una nueva copia de respaldo disponible en el depósito de Amazon S3.

Procedimiento

1. En la interfaz del usuario de CDRS, seleccione **Protection > VM Protection** en el panel de navegación.

   Las máquinas virtuales protegidas existentes aparecen en el panel derecho. En la columna **Rapid recovery image**, se indica si la máquina virtual está habilitada para una recuperación rápida.

2. Seleccione una o más máquinas virtuales y haga clic en **Create Rapid Recovery Image**.

Resultados

- CDRS crea la AMI y elimina cualquier AMI previa para una copia anterior.

- Puede verificar los resultados mediante el análisis de la columna **Rapid recovery image**.
- Puede desactivar la recuperación rápida para una máquina virtual; para ello, selecciónela y haga clic en **Disable Rapid Recovery Image**.
- Puede monitorear el estado de protección y su progreso mediante el análisis de la columna **Protection status**.

Realización de una prueba de DR o conmutación por error de una sola máquina virtual

En este procedimiento, se describe cómo realizar una prueba de DR o conmutación por error en una única máquina virtual utilizando la interfaz del servidor de Cloud DR.

Antes de comenzar

Para realizar una prueba de DR o conmutación por error de una máquina virtual mediante la interfaz del servidor de Cloud DR, debe tener instancias de máquinas virtuales que cuenten con el software de respaldo en las instalaciones y con la copia en la nube.

Para garantizar una conmutación por error exitosa y prepararse mejor para un desastre, las mejores prácticas recomiendan probar varios escenarios de recuperación ante desastres. Después de realizar una prueba de DR, puede promover la prueba a una conmutación por error.

Cuando ocurre un error operacional o un desastre en las instalaciones, puede conmutar una máquina virtual a la nube pública. Cuando se resuelve el problema en las instalaciones, puede conmutar la máquina virtual nuevamente al ambiente en las instalaciones.

Nota

Al realizar conmutaciones por error, debe conmutar las máquinas virtuales en el orden correcto para garantizar el funcionamiento continuo de los servidores y las aplicaciones.

Procedimiento

1. En la interfaz del usuario de servidor de Cloud DR, seleccione **Recovery > VM Recovery**.

   También puede abrir la página **VM Recovery** desde el tablero al hacer clic en **See All** en el panel **Recovery**.

   Se abre la página **VM Recovery**.

2. Seleccione la máquina virtual que desee recuperar y haga clic en **DR Test** o **Failover**.

   Si hace clic en **Failover** y nunca se ha probado la máquina virtual, un mensaje le pregunta acerca de esta condición. Se recomienda ejecutar una prueba de DR antes de implementar una conmutación por error. El mensaje también recomienda que cierre la máquina virtual de producción para evitar una posible pérdida de datos causada por el acceso accidental del usuario.

   Haga clic en **Select Copy** para continuar.

3. En la ventana **Copy and Network** , seleccione la copia de VM y la red donde desee iniciar la instancia de EC2.

En la sección **Advanced Options**, en la parte inferior de la ventana, se indica el tipo de instancia de EC2 autoseleccionada y el grupo de seguridad que se usará para el proceso de recuperación.

4. Si no desea utilizar el tipo de instancia de EC2 autoseleccionada o el grupo de seguridad,, expanda **Advanced Options** y seleccione un tipo de instancia de EC2 alternativa y uno o más grupos de seguridad.
5. Haga clic en **Start DR Test** o **Start Failover**.

Resultados

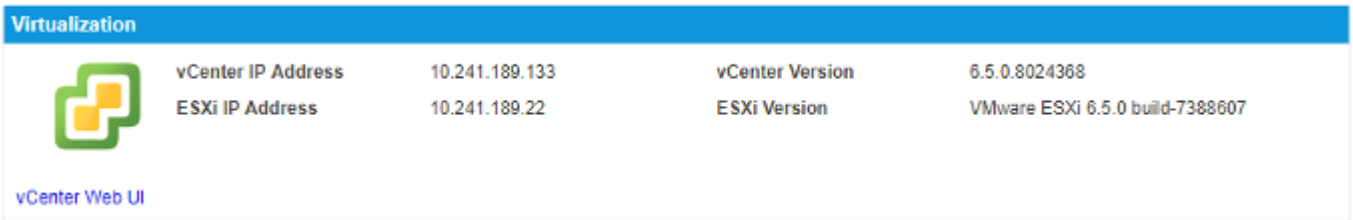
Comienza el proceso de recuperación y es posible monitorear el progreso en la página **DR Activities**. Durante el proceso de recuperación:

1. Si la máquina virtual no está habilitada para la recuperación rápida, se inicia una instancia de servicio de restauración temporal en cada región donde se necesita recuperación. Esta instancia realiza la hidratación durante la recuperación y finaliza automáticamente después de 10 minutos de tiempo de inactividad.
2. El servidor de Cloud DR, a continuación, convierte el VMDK en AMI y se inicia una instancia de EC2 que se basa en AMI.
3. Cuando se ejecuta la instancia de EC2, el servidor de Cloud DR elimina el VMDK y AMI.

Panel Virtualization

En el panel **Virtualization** , se muestra información sobre el ambiente virtual interno en el dispositivo, como la dirección IP y la versión de vCenter Server y host ESXi.

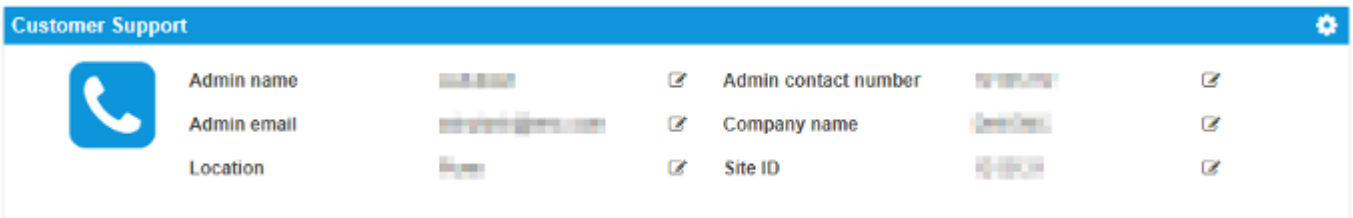
Figura 8 Panel **Virtualization** en la página **Home** de ACM



Cambiar información de contacto del cliente

En el panel **Customer Support**, se muestra la información de contacto del sitio y el contacto del administrador. Para ver el valor completo de un elemento, pase el cursor sobre él.

Figura 9 Panel **Customer Support** en la página **Home** de ACM.



Procedimiento

1. En el panel **Customer Support**, haga clic en el icono **Edit** junto al valor que desee cambiar.

2. Escriba un nuevo valor:
   - **Admin Name**: Escriba el nombre del administrador y haga clic en **Save**.
   - **Admin Number**: Escriba el número de teléfono del administrador y haga clic en **Save**.
   - **Admin Email**: Escriba la dirección de correo electrónico del administrador y haga clic en **Save**.
   - **Company Name**: Escriba el nombre de la empresa y haga clic en **Save**.
   - **Location**: Escriba la ubicación de IDPA y haga clic en **Save**.
   - **Site ID**: Escriba el ID del sitio de IDPA y haga clic en **Save**.

   Puede verificar su número de ID de sitio en el sitio web de Soporte en línea:

   a. Inicie sesión en el sitio web de Soporte en línea con sus credenciales.
   b. Seleccione **Centro de servicios**.
   c. En la página Centro de servicios, debajo del área de sitios y contratos, haga clic en **Administrar un sitio**.
   d. Asegúrese de que el sitio donde esté instalado el sistema de almacenamiento figure en el área Mis sitios.

Nota

También puede buscar un sitio y agregarlo a la lista Mis sitios. Si no está disponible un ID de sitio o si el ID de sitio correcto no aparece en la lista, debe notificar al representante de campo local para solicitar uno.

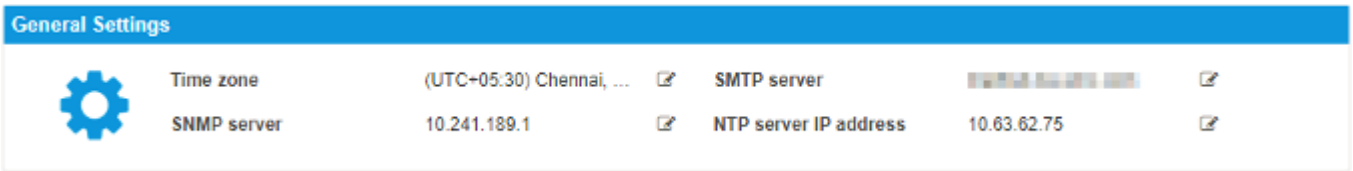
Resultados

Cualquier información nueva que se proporciona se actualiza para el nodo del servidor de respaldo.

Cambiar ajustes generales del sistema

En el panel **General Settings**, se muestra la configuración básica, incluida la configuración de redes y la hora. Para ver el valor completo de un elemento, pase el cursor sobre él.

Figura 10 Panel **General Settings** en la página **Home** de ACM



Procedimiento

1. En el panel **General Settings**, haga clic en el icono **Edit** junto al valor que desee cambiar.
2. Seleccione o escriba un nuevo valor:
   - **Time Zone**: Seleccione la zona horaria de la lista y haga clic en **Save**. Se actualiza la zona horaria para Avamar, Data Domain, nodos de DP Advisor y nodos de Search, ACM y el servidor de host de vCenter.

AVISO

Si se cambia esta configuración, el nodo de Data Domain se reinicia automáticamente.

- **SMTP**: Escriba la dirección IP del servidor SMTP y haga clic en **Save**. Se actualiza la dirección IP del servidor SMTP para los nodos de Avamar y Data Domain y el servidor de host de vCenter.

  AVISO

  Si se cambia esta configuración, los servicios de Avamar MCS y Backup Scheduler se reinician automáticamente. Asegúrese de que no haya ningún respaldo en ejecución en el nodo de Avamar antes de cambiar esta configuración.

- **SNMP**: Escriba la dirección IP del servidor SNMP y haga clic en **Save**. Se actualiza la dirección IP del servidor SNMP para los nodos de Avamar y Data Domain, y para el servidor de host de vCenter.
- **NTP**: Escriba la dirección IP del servidor NTP y haga clic en **Save**. Se actualiza la dirección IP del servidor NTP para los nodos de Avamar, Data Domain, DP Advisor y Search, ACM y el servidor de host de vCenter.

  Nota

  El servidor NTP debe especificarse según la dirección IP. No utilice un nombre de servidor en este campo.

3. Para cambiar ACM DNS, siga este paso:

   a. Edite el archivo `etc/resolv.conf` y, a continuación, especifique la dirección IP del servidor DNS del cliente y el nombre de dominio.

   Por ejemplo, cuando el ambiente del cliente tiene un servidor DNS público con una dirección IP de 10.254.66.23 y el nombre de dominio es mycompany.com, el archivo `/etc/resolv.conf` contiene las siguientes entradas:

   Nota

   El siguiente resultado es un ejemplo, no contiene el nombre de dominio real ni las direcciones de nameserver. El cliente debe proporcionar estos valores.

   ```
   search mycompany.com
   nameserver 10.254.66.23
   nameserver 192.168.100.100
   ```

   Nota

   Asegúrese de que la entrada para el servidor DNS público aparezca antes que el servidor DNS privado. Si el servidor DNS privado aparece primero, se producirá un error en la integración de DPA con el sistema Data Domain.

Configuración del ambiente de LDAP externo

De forma predeterminada, la aplicación tiene la configuración de LDAP interno. Puede cambiar la configuración predeterminada para un ambiente de LDAP externo.

Nota

Asegúrese de cumplir con los siguientes requisitos de contraseña de LDAP mientras configura el ambiente de LDAP externo:

- Use solo los siguientes caracteres:
  - Letras (`A-Z`, `a-z`)
  - Números (`0-9`)
  - Punto (`.`)
  - Guion (`-`)
  - Guion bajo (`_`)
- Debe tener al menos un carácter especial compatible.
- No debe tener más de 20 caracteres.

Procedimiento

1. Seleccione el **tipo de LDAP**.
2. Seleccione **Secure LDAP** para especificar si el protocolo LDAP es seguro.
3. Escriba el **hostname del servidor**.
4. Escriba el **nombre de dominio**.

   Nota

   El nombre de dominio puede tener caracteres alfanuméricos y caracteres especiales (`-`, `_`, `.`, `=` y `,`).

5. Escriba el **nombre de usuario de consulta**.

   Nota

   El nombre de usuario de consulta puede tener caracteres alfanuméricos y caracteres especiales (`-`, `_`, `.`, `=`, `,` y `@`).

6. Escriba la **contraseña de consulta**.

   Nota

   La contraseña de consulta debe tener un mínimo de 9 a 20 caracteres y contener al menos una letra minúscula, una letra mayúscula, un dígito y cualquiera de estos caracteres especiales: `-`, `_`, y `.`.

7. Escriba el **número de puerto**.
8. Haga clic en **Validate** para seleccionar la validación de los detalles de LDAP.
9. Haga clic en **Submit** y, luego, en **Close**.

   La configuración se ha actualizado a un ambiente de LDAP externo.

Nota

Después de configurar LDAP en el ambiente externo, no puede volver a la configuración predeterminada (interna).

10. Haga clic en **Close**.

Apagado de IDPA

Procedimiento

1. Use el protocolo SSH para iniciar sesión en la IP de AVE en el tablero ACM. Use "admin" como usuario y la contraseña común para el dispositivo.
2. Desde el inicio de sesión raíz, ejecute el comando **/usr/local/avamar/bin/avinstaller.pl--checkPrcessingPackage** para comprobar si hay algún paquete de instalación en curso en AVE o no. Si hay alguno, espere hasta que se complete la instalación del paquete.

```
root@xxxxxxx:/home/admin/#: /usr/local/avamar/bin/
avinstaller.pl --checkPrcessingPackage
roo@xxxxxxx:/home/admin
```

3. Ejecute el comando **dpnctl status all**. Examine la salida y asegúrese de que todos los servicios importantes de servidor de respaldo estén funcionando como se muestra en la siguiente captura de pantalla. Si no, póngase en contacto con el servicio al cliente.

```
admin@xxxxxxx~/>: dpcnt1 status all
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: gsan status: up
dpnctl: INFO: MCS status: up
dpnctl: INFO: emt status: up
dpnctl: INFO: Backup scheduler status: up
dpnctl: INFO: Maintenance windows scheduler status: enabled
dpnctl: INFO: Unattended startup status: disabled
dpnctl: INFO: avinstaller status: up
dpnctl: INFO: ConnectEMC status: up
dpnctl: INFO: ddrmaint-service status: up
```

4. Ejecute el comando **mccli checkpoint show** para verificar todos los puntos de control disponibles en el sistema Avamar. Tome una captura de pantalla de la salida de la ejecución de este comando. La captura de pantalla será útil en las etapas posteriores del procedimiento de apagado.

```
admin@xxxxxxx:/home/admin/>:mccli checkpoint show
0,23000,CLI command completed successfully
Etiqueta                  Hora               Validado
Eliminable
cp. 20180523033106 2018-05-23 09:01:06 IST Validated   No
cp. 20180523033444 2018-05-23 09:04:44 IST             No
cp. 20180523054859 2018-05-23 11:18:59 IST             No
```

5. Ejecute el comando **mccli checkpoint create--override_maintenance_scheduler** para crear un punto de control en AVE.

```
admin@xxxxxxx:/home/admin/>mccli checkpoint
create --override_maintenance_scheduler
0,22624, Starting to create a server checkpoint.
```

6. Después de que se ejecute el comando anterior, ejecute el comando **mccli checkpoint show** en AVE otra vez para ver la etiqueta del punto de control que se creó recientemente y que se asignó al punto de control que inició en el paso

anterior. La entrada puede tardar en reflejarse en la salida de este comando (es posible que deba repetir este comando 2 o 3 veces). La entrada del punto de control recién creado se puede validar a partir del registro de fecha y hora asociado con las entradas. En la siguiente captura de pantalla, cp. 20180523033444 es la etiqueta del punto de control recién creado.

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Etiqueta                  Hora               Validado
Eliminable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST              Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

7. Ejecute el siguiente comando **mccli checkpoint validate --cptag=<cp_tag_of_new_checkpoint> --override_maintenance_scheduler** para validar el punto de control.

```
admin@xxxxxxx:/home/admin/>: mccli
checkpoint validate --cptag=cp.20180523033444 --
override_maintenance_scheduler
0,22612,Starting to validate a server checkpoijnt
Atributo    Valor
tag         cp. 20180523033444
type        Full
```

8. Ejecute el comando **mccli checkpoint show** para verificar el estado del proceso de validación del punto de control. La pantalla mostrará **In Progress** por un período prolongado de tiempo. Espere hasta que la pantalla muestre el estado **Validated** para la etiqueta del punto de control.

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Etiqueta                  Hora               Validado
Eliminable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST In Progress  Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

```
admin@xxxxxxx:/home/admin/>:
mccli checkpoint show
0,23000,CLI command completed successfully
Etiqueta                  Hora               Validado
Eliminable
cp. 20180523033106  2018-05-23 09:01:06 IST Validated     No
cp. 20180523033444  2018-05-23 09:04:44 IST Validated    Yes
cp. 20180523054859  2018-05-23 11:18:59 IST              No
cp. 20180523055705  2018-05-23 11:27:05 IST              No
```

9. Desde el inicio de sesión raíz, ejecute el comando **avmaint hfscheckstatus <checkpoint_tag> --ava** para verificar el estado del trabajo. Si es necesario, ejecute el comando **avmaint hfscheck --checkpoint=<checkpoint tag> --ava** para realizar un hfscheck en el punto de control. Espere hasta que el comando de estado de trabajo hfscheck anterior tenga un estado "completed".

```
root@xxxxxxx:/home/admin/#:avmaint hfscheckstatus cp.
20180524033103 --ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheckstatus
nodes-queried="1"
nodes-replied="1"
```

```
nodes-total="1"
checkpoint="cp.20180524033103"
status="waitcomplete"
type="full"
checks="full"
elapsed-time="114"
start-time="1527154524"
end-time="0"
check-start-time="1527154524"
check-end-time="1527154562"
generation-time="1527154565"
stripes-checking="31"
stripes-completed="31"
offline-stripes="0"
minutes-to-completion="100.00">
<hfscheckerrors/>
</hfscheckstatus>
root@xxxxxxx:/home/admin/#:
```

```
root@xxxxxxx:/home/admin/#:avmaint hfscheck cp.20180524033103 --
ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheck
checkpoint="cp.20180524033103"
status="waitcgsan"
type="full"
checks="full"
elapsed-time="73"
start-time="1527154451"
end-time="0"
check-start-time="0"
check-end-time="0"
generation-time="1527154524"
percent-complete="0.00">
<hfscheckerrors/>
</hfscheck>
```

```
root@xxxxxxx:/home/admin/#:avmaint hfscheckstatus cp.
20180524033103 --ava
<?xml version="1.0" encoding-"UTF-8" standalone-"yes"?>
<hfscheckstatus
nodes-queried="1"
nodes-replied="1"
nodes-total="1"
checkpoint="cp.20180524033103"
status="completed"
result="OK"
type="full"
checks="full"
elapsed-time="103"
start-time="1527154451"
end-time="1527154554"
check-start-time="1527154524"
check-end-time="1527154554"
generation-time="1527154651"
stripes-checking="31"
stripes-completed="31"
offline-stripes="0"
percent completion="100.00">
<hfscheckerrors/>
</hfscheckstatus>
```

10. Ejecute el comando **dpcntl stop schedd** para detener todo el trabajo de respaldo que será programado por AVE (los trabajos actuales continuarán ejecutándose).

```
admin@xxxxxxx:~/>: dpnctl stop sched
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
```

```
dpnctl: INFO: Suspending backup scheduler...
dpnctl: INFO: Backup scheduler suspended.
```

11. Ejecute el comando **dpnctl stop maint** para detener los servicios de mantenimiento que se ejecutan en Avamar.

```
admin@xxxxxxx:~/>: dpnctl stop maint
Identity added: /home/admin/.ssh/admin_key (/home/admin/.ssh/
admin_key)
dpnctl: INFO: Suspending maintenance windows scheduler...
dpnctl: INFO: Maintenance windows scheduler suspended.
```

12. Desde el inicio de sesión raíz, ejecute el comando **cplist** y verifique lo siguiente:
    a. Compruebe si el punto de control hfschecked está presente en 36 horas.
    b. Compruebe si hay una entrada de hfs para al menos un punto de control que se haya creado en las últimas 36 horas.

```
root@xxxxxxx://ust/local/avamar/bin/#: cplist
cp. 20180524033103 Thu May 24 09:01:03 2018 valid hfs --- nodes
1/1 stripes  32
cp. 20180524033441 Thu May 24 09:04:03 2018 valid hfs --- nodes
1/1 stripes  32
```

13. Ejecute el comando **avmaint sessions** en AVE. Esto detiene todas las sesiones activas en Avamar. Enumerará todas las sesiones que se estén ejecutando actualmente en AVE. Para cancelar cada sesión, seleccione **sessionid** y ejecute el comando **avmaint kill <sessionid>'**. Haga esto para cada sesión hasta que no se encuentren entradas de sesión en AVE.

```
admin@xxxxxxx://>: avmaint sessions
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<nodesessionlist count="1">
<sessionlist
id="0.0"
count="1"
<session
numthreads="1"
type="avtarbackup"
ndispatchers="1"
expires="1532240626"
domain=""
workorderid="MOD-1527056601340"
pidnum="1001"
numconns="1"
path="/clients/acmpun059.lss.emc.com"
starttime="1527056651"
encrypt=="tls-sa"
dispatcher0="xxxxxxxxxxxxxx"
sessionid="9152705660134709"
root="/"
pluginid="Unix"
encrypt-strength="high"
clientid="86752318de80049804395b0756fde3fa034a9846"
user=""
clientip=xxxxxxxxxxxxx>
<host
numprocs="4"
speed="16777200"
osuser="root"
name="xxxxxxx"
memory="32175">
<build
msgversion="13-10"
time="06:46:59"
appname="avtar"
zlibversion="1.2.8"
lzoversion=1.08 Jul 12 2002"
```

```
date "Mar 22 2018"
appversion="7.5.101-101_HF294929"
processortype="x86_64"
osversion="SLES-64"
sslversion="TLSv1 OpenSSL 1.0.2a-fips 19 Mar 2015
osname="Linux"/>
```

```
admin@xxxxxxx://>: avmaint kill 9152705692533109
kill: killed 9152705692533109
```

```
admin@xxxxxxx:/home/admin/>: avmaint sessions
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<nodesessionlist count="1">
<sessionlist
id="0.0"
count="0"/>
</nodesessionlist>
```

14. Desde el inicio de sesión raíz de Avamar, ejecute **avmaint cpstatus** para verificar que no haya puntos de control en progreso. Verifique que todos los puntos de control enumerados tengan un estado “completed”. Espere a que se completen los puntos de control si se están ejecutando.

```
roor@xxxxxxx://#: avmaint cpstatus
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<cpstatus
generation-time="1527099528"
tag="cp.20180523055705"
status="completed"
stripes-completed="32"
stripes-total="32"
start-time="1527055025"
end-time="1527055044"
result="OK"
refcount="1"/>
```

15. Ejecute **avmgr getb --path=/MC_BACKUPS --mr=1 --format=xml** para verificar que el MCS se haya vaciado en las últimas 12 horas. Puede verificar el tiempo real del vaciado de MCS ejecutando la entrada **t.pl <time_tag>** (ejecute en el directorio /usr/local/avamar/bin). Si MCS no se ha vaciado en las últimas 12 horas, ejecute **mcserver.sh- -flush**' para vaciar el MCS en AVE.

```
admin@xxxxxxx:~/>: avmgr getb  --path=/MC_BACKUPS --mr=1 --
format=xml
1 Request succeeded
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<backuplist version="3.0">
<backuplistrec flags="32768001" labelnum="418" label=""
created="157174902"
roothash="587c90ceea90e7523366025b3955a8ed142170f"
totalbytes="48514156.00"
ispresentbytes="0.00" pidnum="1001" percentnew"0" expires="0"
created_prectime="0x1d3f371fd3ffb5a" partial="0"
retentiontype="daily,weekly,monthly,yearly
backuptype="full" ddrindex="0" locked="1" direct_restore="1"
tier="0"
appconsistent="not_available"/>
</backuplist>
```

```
admin@xxxxxxx:~/>: mcserver.sh--flush
=== BEGIN === check.mcs (preflush)
check.mcs     passed
=== PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Adminstrator Server Flushed.
```

```
admin@xxxxxxx:~/>: avmgr getb  --path=/MC_BACKUPS --mr=1 --
format=xml
1 Request succeeded
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
```

```
<backuplist version="3.0">
<backuplistrec flags="32768001" labelnum="419" label=""
created="157178362"
roothash="5876c90ceea90e7523366025b3955a8ed1422170f"
totalbytes="48514156.00"
ispresentbytes="0.00" pidnum="100" percentnew"0" expires="0"
created_prectime="0x1d3f371fd3ffb5a" partial="0"
retentiontype="daily,weekly,monthly,yearly
backuptype="full" ddrindex="0" locked="1" direct_restore="1"
tier="0"
appconsistent="not_available"/>
</backuplist>
```

```
admin@xxxxxxx:~/>:/usr/local/avamar/bin/>: t.pl 1527178362
local: Thu May 24 21:42:42 2018   gmt: Thu May 24 16:12:42 2018
```

```
admin@xxxxxxx:~/>: mcserver.sh--flush
=== BEGIN === check.ms (preflush)
check.mcs
===PASS === check.mcs PASSED OVERALL (preflush)
Flushing Administrator Server...
Administrator Server Flushed
```

16. En el directorio /usr/local/avamar/bin, ejecute **hfscheck_kill** para cancelar los trabajos de hfscheck (si todavía hay alguno en ejecución).

```
admin@xxxxxxx:/usr/local/avamar/bin/#: hfscheck_kill
Using /usr/local/avamar/ver/probe.xml
```

17. Ejecute el comando **avmaint gckill --ava** para cancelar todos los trabajos de recolector de elementos no utilizados.

```
admin@xxxxxxx:/usr/local/avamar/bin/#: avmaint gckill --ava
```

18. Ejecute el comando **dpnctl shutdown --precheck** para comprobar si se cumplen todos los requisitos de apagado.

```
admin@xxxxxxx:~/>: dpnctl shutdown --precheck
Identity added /home/admin/.ssh/admin_key)
dpnctl: INFO: Checking for validated checkpoint
dpnctl: INFO: found the most recently validated checkpoint: cp.
20180523033444 at
'Wed May 23 03:34:44 2018 UTC'
dpnctl: INFO: VALIDATED CHECKPOINT PASSED
dpnctl: INFO:
[###############-----------------------------------20%]
dpnctl: INFO: Starting MCS flush check
dpnctl: INFO: Last MCS flush at 'Wed May 23 15:45:02 2018'
dpnctl: INFO: LAST MCS PASSED
dpnctl: INFO:
[###############-----------------------------------30%]
dpnctl: INFO: Checking for file system and gsan percentage
dpnctl: INFO: FS/GSAN PERCENTAGE PASSED
dpnctl: INFO:
[###############-----------------------------------50%]
dpnctl: INFO: GSAN tasks: idle
dpnctl: INFO: Checking for hfscheck.
dpnctl: INFO: No hfsceck maintenance task is running.
dpnctl: INFO:
[###############-----------------------------------70%]
dpnctl: INFO: Checking for GC.
dpnctl: INFO: No GC task is running.
dpnctl: INFO:
[###############-----------------------------------80%]
dpnctl: INFO: Checking for active sessions (backup/restore).
dpnctl: INFO: No backup/restore is running.
dpnctl: INFO:
[###############-----------------------------------90%]
dpnctl: INFO: Checking for active checkpoint.
dpnctl: INFO: No checkpoint task is running.
```

```
dpnctl: INFO:
[##############----------------------------------100%]
```

19. Realice la limpieza del sistema de archivos mediante la ejecución del siguiente comando CLI en el administrador de Data Domain:

```
filesys clean status
```

20. Verifique que se sincronicen las contraseñas. Al cambiar una contraseña para un componente, la interfaz del usuario de ACM muestra el mensaje de error de sincronización de la contraseña. Revise cada panel en el tablero y asegúrese de que todas las contraseñas estén sincronizadas. Si alguna contraseña no está sincronizada, el proceso de apagado no puede comenzar. Para permitir que ACM recopile información del estado de los componentes, debe actualizar la contraseña almacenada en la interfaz del usuario de ACM para que coincida. Para actualizar una contraseña no sincronizada, haga clic en el texto del error.
21. En la pestaña **Home** del tablero, haga clic en el icono **Shutdown Appliance**.
22. Escriba la contraseña del administrador, haga clic en **Authenticate**y luego haga clic en **Yes**.
23. Haga clic en **Cerrar sesión**.

⚠ PRECAUCIÓN

Pasará mucho tiempo (aproximadamente 45 minutos) entre que el ACM se apague y el sistema se apague físicamente.

Mientras se está apagando el dispositivo, la pantalla **Login** muestra un mensaje que indica que se está apagando. Para ver el estado, inicie sesión en ESX para monitorear el apagado.

Health

En la pestaña **Health** se muestra información del estado y las alertas para los siguientes componentes de hardware de IDPA:

- Servidores DP4400
- vCenter

IDPA utiliza Secure Remote Services para enviar automáticamente los eventos críticos y graves a Servicio al cliente para la solución de problemas. Se abre un vale de soporte en función de los eventos que se reciben. Los eventos críticos y graves se envían a Servicio al cliente después de que hayan transcurrido 30 minutos o cuando se acumulan 30 eventos (lo que ocurra primero).

De manera predeterminada, todos los eventos se eliminan después de 30 días. Si no se produjeron eventos en el período de tiempo seleccionado, los paneles **Event Summary** y **Event Details** indican que no hay datos disponibles.

Event Summary

En el panel **Event Summary** se muestra un resumen de los eventos de estado en el dispositivo, agrupados por **dispositivo** y **gravedad**.

Para cambiar el período de tiempo para el que se muestran los eventos, seleccione una opción del cuadro **Event summary for**. Al seleccionar **Today**, se enumeran los eventos que han ocurrido desde la medianoche hasta el presente.

Para mostrar solo eventos para un dispositivo específico o de una gravedad específica en el panel **Event Details**, haga clic en la parte correspondiente en el gráfico.

Event Details
En el panel **Event Details** se muestra una lista paginada de los eventos de estado en el dispositivo. Use los cuadros **Device** y **Severity** para filtrar la lista por dispositivo, gravedad o ambos. Para leer información más detallada sobre un evento, haga clic en su entrada de tabla. Para exportar la lista como un archivo CSV, haga clic en el icono de CSV.

Solución de problemas
Si un componente crítico de la función de monitoreo del estado no está funcionando, los paneles indican que el servicio está inactivo y se muestra un mensaje de error en la parte superior de la página. Para obtener más información acerca de cómo resolver problemas relacionados con la pestaña **Health**, consulte Solución de problemas del monitoreo de estado en la página 50.

Upgrade

La pestaña **Upgrade** permite que un administrador actualice el software de IDPA. Consulte Actualización del software de IDPA en la página 43 para obtener más información.

Acceso a componentes con un navegador

Además de hacer clic en los vínculos en los paneles de ACM, puede acceder a la interfaz del usuario para los componentes individuales; para ello, navegue hasta la ubicación de red correspondiente y escriba el nombre de usuario y la contraseña.

En cada una de las siguientes secciones, *<component_ip>* se refiere a la dirección IP del componente. Las credenciales para Search y IDPA System Manager están determinadas por la configuración LDAP.

Nota

Asegúrese de estar utilizando Flash versión 27.0.0.183 o posterior para acceder al cliente web de vCenter.

Tabla 4 Acceso a los componentes

Componente	Ubicación	Nombre de usuario
Avamar Client Manager	`https://<component_ip>/aam`	`MCUser`
Interfaz del usuario de Avamar	`https://<component_ip>/mcui`	`MCUser`
Inicio de sesión de protocolo SSH de Avamar		`admin`
Interfaz del usuario de Data Domain	`https://<component_ip>`	`sysadmin`
Interfaz del usuario de IDPA System Manager	`https://<component_ip>`	`<username>@<domain>`

Tabla 4 Acceso a los componentes (continuación)

Componente	Ubicación	Nombre de usuario
		Nota Si el LDAP externo no se ha configurado, entonces el nombre de usuario predeterminado es `idpauser`.
Interfaz del usuario de DP Advisor	`https://<component_ip>:90502/dpaui/jsp`	`administrador`
Interfaz del usuario de Search	`https://<component_ip>/admin/#/login`	`<username>@<domain>` **Nota** Si el LDAP externo no se ha configurado, entonces el nombre de usuario predeterminado es `idpauser`.
vCenter Web Client	`https://<component_ip>`	`idpauser`

Cuentas de usuario para los componentes

La configuración de IDPA utiliza las cuentas de usuario en Tabla 5 en la página 38. De forma predeterminada, estas cuentas utilizan la contraseña común de IDPA . Para obtener información sobre cómo cambiar las contraseñas de componente, consulte Cambio de contraseñas y sincronización de los componentes en la página 39.

Tabla 5 Componente y asignación de la cuenta de usuario

Componente	Uso de SSO	Nombre de usuario	Contraseña
ACM	No	root	Contraseña común proporcionada durante la configuración de DP4400.
IDPA System Manager (si no está configurado el LDAP externo)	No	idpauser	Contraseña común proporcionada durante la configuración de DP4400.
IDPA System Manager (si está configurado el LDAP externo)	No	Credenciales de LDAP correspondientes	Contraseña de LDAP externo, según corresponda.
Avamar	Sí	N/C	SSO se encargará de este registro automáticamente.

Tabla 5 Componente y asignación de la cuenta de usuario (continuación)

Componente	Uso de SSO	Nombre de usuario	Contraseña
Data Domain	No	sysadmin	Contraseña común proporcionada durante la configuración de DP4400.
Data Protection Advisor	No	administrator	Contraseña común proporcionada durante la configuración de DP4400.
Search	Sí	N/C	SSO se encargará de este registro automáticamente.
CDRA	No	admin	Contraseña común proporcionada durante la configuración de DP4400.
CDRS	No	admin o monitor	Contraseña configurada durante la implementación de CDR.
vCenter	No	idpauser	Contraseña común proporcionada durante la configuración de DP4400.
ESXi	No	idpauser	Contraseña común proporcionada durante la configuración de DP4400.

Cambio de contraseñas y sincronización de los componentes

El cambio de contraseña de usuario con un solo clic es una de las nuevas funciones presentadas en DP4400. Se recomienda que use la función para cambiar la contraseña, ya que cambia las contraseñas para todos los componentes de IDPA.

Nota

No se recomienda cambiar las contraseñas de los componentes individuales. Debido a cualquier circunstancia imprevista, si tiene que cambiar las contraseñas de los componentes individuales, consulte la siguiente sección.

Cambio de contraseñas para los componentes individuales

Algunos cambios para la configuración y las contraseñas de un componente requieren la actualización de la configuración de otros componentes.

Cambiar una contraseña para un componente hace que la interfaz del usuario de ACM muestre el mensaje de error `password out of sync`. Para permitir que ACM recopile información del estado de los componentes, debe actualizar la contraseña almacenada en la interfaz del usuario de ACM para que coincida. Para actualizar una contraseña no sincronizada, haga clic en el texto del error.

Configuración de Data Domain

Actualización de la contraseña de Data Domain

Para obtener información sobre cómo cambiar la contraseña de la cuenta `sysadmin` de Data Domain, consulte *Data Domain Operating System: guía de administración*. Después de cambiar la contraseña de la cuenta `sysadmin`, inicie sesión en DP Advisor y actualice las credenciales de SSH de Data Domain para que coincidan.

AVISO

Actualice las credenciales de SSH de Data Domain en DP Advisor inmediatamente. No hacerlo puede provocar el bloqueo de cuenta cuando DP Advisor intenta conectarse repetidamente con la contraseña anterior.

Después de actualizar la contraseña en DP Advisor, inicie sesión en ACM y actualice la contraseña de **Protection Storage** para que coincida.

Nota

No cambie la contraseña de usuario de DD Boost antes de configurar CDRA desde el tablero.

Configuración de Avamar

Actualización de las contraseñas de Avamar

Avamar utiliza varias cuentas de usuario, incluyendo `MCUser`, `viewuser`, servidor `root`, SO `admin`, y SO `root`. IDPA requiere que las cuentas del SO `admin` y del SO `root` utilicen la misma contraseña. `MCUser`, `viewuser` y las cuentas del servidor `root` también deben compartir una contraseña, que puede ser distinta de la contraseña del SO `admin` y el SO `root`. Para obtener más información sobre cómo cambiar la contraseña de Avamar, consulte *Avamar Guía de administración*.

Después de cambiar la contraseña para cualquier cuenta de Avamar, inicie sesión en ACM y actualice la contraseña de **Backup Server** para que coincida.

Si cambia la contraseña de la cuenta `MCUser`, actualícela en la interfaz del usuario de administrador de Search. Para obtener más información sobre cómo cambiar la contraseña de Avamar para Search, consulte *Guía de instalación y administración de Data Protection Search*.

Si cambia la contraseña de la cuenta `viewuser`, actualícela en la interfaz del usuario de DP Advisor. Para obtener más información sobre cómo cambiar la contraseña de Avamar en DP Advisor, consulte *Data Protection Advisor Guía de instalación y administración*.

Actualización de la contraseña del usuario de DD Boost

Después de cambiar la contraseña para la cuenta de Data Domain`DDBoostUser`, inicie sesión en la GUI de **Avamar Administrator**. Edite la configuración del sistema Data Domain y actualice la contraseña de usuario de DD Boost para que coincida. Para obtener más información, consulte el procedimiento "Edición de un sistema Data Domain" en la *Avamar Guía de administración*.

Nota

No cambie la contraseña de usuario de DD Boost antes de configurar CDRA desde el tablero.

Configuración de DP Advisor

Actualización de las contraseñas de DP Advisor

Para cambiar la contraseña de cuenta `administrator` de DP Advisor o la contraseña `root`, debe iniciar sesión y cambiar esa contraseña para cada nodo DP Advisor. Para obtener más información sobre cómo cambiar una contraseña en DP Advisor, consulte la *Data Protection Advisor Guía de instalación y administración*.

Después de cambiar la contraseña en todos los nodos, inicie sesión en ACM y actualice la contraseña de **Reporting and Analytics** para que coincida.

Actualización de la cadena de comunidad de SNMP de Data Domain.

Si se cambia la cadena de comunidad de su valor predeterminado de *public*, DP Advisor debe actualizarse para reflejar el cambio.

1. Inicie sesión en Data Domain y cambie la cadena de comunidad con el siguiente comando, donde *<community_string>* es la nueva cadena y *<Dpa_DC_Agent_IP>* es la dirección IP de la máquina virtual de Data Collection Agent.

   snmp add rw-community hosts <community_string> <Dpa_DC_Agent_IP>

2. En el panel **Reporting and Analytics** de ACM, haga clic en el vínculo **Reporting and Analytics Web UI**.
3. Haga clic en **Manage Credentials** en la página **Admin** > **System**.
4. Seleccione **EMC Data Domain Credential** y actualice la cadena de comunidad para que coincida.

Configuración de DPSearch

Actualización de la contraseña de DPSearch

Para cambiar la contraseña de `root` del SO Search, debe iniciar sesión y cambiar la contraseña de `root` del SO para cada nodo de Search. Para obtener más información sobre cómo cambiar la contraseña de `root` del SO, consulte la *Guía de instalación y administración de Data Protection Search*.

Después de cambiar la contraseña de la cuenta `root` del SO Search, inicie sesión en ACM y actualice la contraseña de **Search** para que coincidan.

Nota

`#`, `?`, `/` y `\` son caracteres no permitidos para las contraseñas nuevas.

Actualización de la configuración de LDAP para DPSearch

Si se cambia la contraseña del usuario de consulta de LDAP, es posible que no se pueda iniciar sesión en la interfaz del usuario del administrador de DPSearch. Para actualizar esta contraseña, consulte los procedimientos a los que se hace referencia en la *Guía de instalación y administración de Data Protection Search*.

1. La primera vez que inicie sesión en un nodo de Search con el protocolo SSH, deberá aceptar el EULA. Para obtener más información, consulte el procedimiento "Inicialización del ambiente de Data Protection Search" en la *Guía de instalación y administración de Data Protection Search*.
2. Después de aceptar el EULA, seleccione la opción `[2] Configure Network Settings` y, a continuación, presione **F9** para salir.

3. Cuando el sistema muestre `Do you want to reboot now? y(es) or n(o):`, escriba **no**.
4. Para actualizar la configuración de LDAP, complete el procedimiento "Actualización de la configuración de LDAP en el script de instalación de administrador de Data Protection Search" en *Guía de instalación y administración de Data Protection Search*.
5. Repita los pasos del 1 al 4 para cada nodo de Search.
6. Inicie sesión en cada nodo de datos de índice de Search con SSH y ejecute el comando **service unicorn restart**.
7. Inicie sesión en el nodo maestro de índice de Search con SSH y ejecute el comando **service unicorn restart**.

CAPÍTULO 3

Actualización del software de IDPA

En este capítulo, se describe cómo actualizar el software de IDPA.

Se abordarán los siguientes temas:

Actualización del software del dispositivo

Actualice el software para IDPA desde la pestaña **Upgrade**.ACM

Una vez que el archivo de actualización de software se descarga y se copia en el directorio `/data01/upgrade`, el archivo de paquete se detecta automáticamente y aparece en **Upgrade Binary Location**.

CAPÍTULO 4

Solución de problemas

Este capítulo contiene información sobre la solución de problemas básica para ayudar a resolver los posibles problemas.

Se abordarán los siguientes temas:

Archivos de registro del sistema

Para ayudar a solucionar problemas, descargue los archivos de registro incluidos para IDPA directamente desde la página de la pestaña **Home**. Seleccione la opción **Download log bundle** desde el icono de paquete de registro disponible en la página de la pestaña **Home** para descargar los archivos de registro. Se guardan los archivos de registro para los componentes especificados en la carpeta `/Downloads/` en el sistema en un formato comprimido.

Nota

El usuario no debe crear ni copiar sus registros en la carpeta `/data01/log_bundle`, ya que esta funcionalidad elimina todos los registros existentes mientras se crea el paquete de registros.

Solución de problemas del inicio

Si una parte del proceso de inicio no se completa automáticamente, se puede resolver el problema manualmente para permitir que el inicio continúe.

Avamar no se inicia
Si Avamar no completa el inicio conéctese al servidor Avamar. Si Avamar informa que GSAN no se ha apagado correctamente, seleccione la opción de revertir al último punto de control.

ACM no se inicia
Si el servicio de ACM no se inicia en un plazo de 2 horas y 15 minutos desde el encendido del dispositivo, uno o varios de los siguientes componentes no están encendidos o no son accesibles en la red:

- Data Domain
- AVE

El componente Data Domain debe estar encendido y debe ser accesible para que el host ESXi esté encendido.

1. Verifique que estén encendidos los componentes que se requieren para la configuración.
2. Verifique que los componentes necesarios sean accesibles en la red. Resuelva cualquier problema de conectividad que encuentre.
   - Si ACM se carga correctamente, omita el resto de este procedimiento. Los nodos Search, los nodos DP Advisor, IDPA System Manager, AVE y el proxy de Avamar se inician automáticamente.
   - Si todos los componentes necesarios se encendieron y son accesibles, pero ACM no se carga, reinicie el servicio ACM:
3. Detenga el servicio `dataprotection_webapp`:
   `service dataprotection_webapp stop`
4. Inicie el servicio `dataprotection_webapp`:
   `service dataprotection_webapp start`

Los nodos Search, los nodos DP Advisor, IDPA System Manager, AVE y el proxy de Avamar se inician automáticamente.

Las máquinas virtuales no se inician

Cuando enciende el botón de encendido presente en el servidor Dell, ACM ejecuta `local.sh (/etc/init.d/local.sh)` internamente y las máquinas virtuales se inician automáticamente. Para iniciar manualmente las máquinas virtuales:

1. Mueva ESXi fuera del modo de mantenimiento de forma manual.

   Nota

   Para ello, inicie sesión en ESX con `idpauser` y seleccione **Exit maintenance mode**.

2. Inicie DataProtection-VCSA mediante la ejecución del script `/etc/init.d/local.sh` en ESXi o encienda la máquina virtual desde el ESXi.
   La máquina virtual DataProtection-ACM se inicia cinco minutos después del inicio de la VM VCSA.
3. Si la máquina virtual DDVE no está encendida, haga clic en el botón **Power** para iniciarla.
   El código espera el estado del sistema de archivos para mostrar y ejecutar.
4. Si AVE no está encendido, inicie la máquina virtual de AVE desde la interfaz del usuario de ESX.
5. Inicie sesión en AVE con credenciales de administrador.
   ACM ejecuta los comandos `dpnctl status all`, `dpnctl start all` y `dpnctl start maint`.
6. Si algo sale mal, ejecute lo siguiente en secuencia y haga clic en el botón **Power on**:
   - DataProtectionSearch Vapp
   - Máquina virtual DPADatastoreServer
   - Máquina virtual DPAApplicationServer
   - VApp DataDomainCloudDR
   - VApp DataProtectionCentral
   - Máquina virtual AVProxy

   Nota

   Compruebe el estado de servicios de DPA mediante la ejecución del comando `/opt/emc/dpa/services/bin/dpa.sh service status` después de iniciar sesión en el servidor de Datastore con su dirección IP, el usuario `root` del SO y su contraseña.

7. Si vApp DPS no arranca, inicie vApp.
8. Comience con los servicios de búsqueda mediante el inicio de sesión en la IP de índice maestro con las credenciales root del SO y con la ejecución de los siguientes comandos:
   a. `service elasticsearch start`
   b. `service search-cis-core start`
   c. `service search-cis-schedule start`
   d. `service search-networker-worker start`
   e. `service search-networker-action start`

f. `service search-avamar-worker start`
g. `service search-avamar-action start`
h. `service search-worker start`
i. `service search-adminapi start`
j. `service search-api start`

9. Inicie sesión en VCSA con las credenciales **idpauser**, seleccione la máquina virtual **AVProxy** y haga clic en el botón **Power on**.
10. Después de que arranque IDPA, inicie dos servicios de Avamar con `dpnctl start emt`.

Cómo agregar un certificado firmado por una CA

ACM incluye un certificado autofirmado, lo cual puede causar que el navegador informe que hay una conexión no segura. Para resolver este problema, reemplace el certificado predeterminado por un certificado firmado por una CA.

Antes de comenzar

- Acceda a la línea de comandos IDPA mediante uno de los siguientes procedimientos:
  - Inicie sesión en vCenter, haga clic con el botón secundario en la máquina virtual DataProtection-ACM y seleccione **Open Console**. Escriba las credenciales de ACM.
  - Conéctese a ACM mediante un cliente SSH para obtener acceso a su dirección IP. Escriba las credenciales de ACM.
- Cambie el directorio a `/root`.

Procedimiento

1. Detenga el servidor Tomcat.

   service dataprotection_webapp stop

2. Respalde el archivo de almacenamiento de claves existente.

   cp /root/.keystore /root/.keystore.bkp
   Use el respaldo si se producen errores en este proceso.

3. Elimine el certificado autofirmado existente del almacenamiento de claves.

   /usr/java/latest/bin/keytool -delete -alias tomcat -storepass changeit

4. Cree un certificado nuevo.

   /usr/java/latest/bin/keytool -genkeypair -v -alias tomcat -keyalg RSA -sigalg SHA256withRSA -keystore /root/.keystore -storepass changeit -keypass changeit -validity 3650 -dname "CN=idpa.companyname, OU=Idpa, O=CompanyName, L=Hopkinton, S=Massachusetts , C=US"

5. Genere un archivo CSR para el almacenamiento de claves.

   /usr/java/latest/bin/keytool -certreq -alias tomcat -keyalg RSA -file /root/ACM_Host.csr -keystore /root/.keystore

6. Obtenga el certificado firmado por una CA en el formato .p7b mediante el contenido de la CSR y guarde el certificado.

7. Importe el certificado nuevo al almacén de claves.

   /usr/java/latest/bin/keytool -import -alias tomcat -file /root/certnew.p7b -keystore /root/.keystore

8. A fin de garantizar que `/usr/local/dataprotection/tomcat/conf/server.xml` esté usando el archivo `/root/.keystore`, seleccione el valor del atributo `keystoreFile` para el conector de HTTP.
9. Verifique los certificados en el almacenamiento de claves.

   /usr/java/latest/bin/keytool -list -keystore /root/.keystore -alias tomcat

10. Reinicie el servidor Tomcat.

    service dataprotection_webapp start

Configuración de AD seguro con certificados autofirmados en IDPA

Si está utilizando AD seguro con certificados autofirmados, la búsqueda no se configura si el certificado autofirmado no está presente en la máquina virtual de búsqueda.

Procedimiento

1. Exporte el certificado de CA raíz.

   Consulte https://support.microsoft.com/en-us/help/555252 para saber cómo exportar el certificado de CA raíz.

2. Inicie sesión en el servidor de la autoridad de certificación raíz o el servidor Active Directory con la cuenta de administrador.
3. Vaya a **Start** > **Run**, escriba `cmd` y presione **Enter**.
4. Para exportar el servidor de la autoridad de certificación raíz con un nuevo nombre de archivo `ca_name.cer`, ejecute `certutil -ca.cert ca_name.cer`.
5. Convierta el certificado a formato PEM de la siguiente manera:
   a. Copie `ca_name.cer` en Search Master.
   b. Ejecute `openssl x509 -in ca_ name.cer -inform der -out ca_name.pem -outform pem`.
   c. Copie este `ca_name.pem` en `/etc/pki/trust/anchors/` en Search Node.
6. Configure LDAP desde el tablero.

Solución de problemas de Avamar

Si hay un problema con Avamar, el panel **Backup server** en el tablero ACM muestra el siguiente estado:

```
Backup Agents Installation in progress...
```

Las posibles causas posibles para este problema incluyen:

- El servicio de Avamar, Avamar o AVE está inactivo.

- No se puede realizar una operación de ping para Avamar.
- Hay un error de coincidencia entre la contraseña del administrador Avamar y la contraseña almacenada en ACM.

El servicio de Avamar está inactivo.
Para iniciar el servicio de Avamar:

1. Mediante un cliente SSH, conéctese al nodo de utilidad de Avamar como usuario administrador.
2. Escriba el comando `dpnctl start all`

Avamar o AVE están inactivos.
Encienda el servidor Avamar o AVE.

No se puede realizar una operación de ping para Avamar
Si no se puede realizar una operación de ping para Avamar, encuentre y resuelva el origen del problema. Las causas posibles incluyen:

- El servidor Avamar está inactivo.
- Hay un problema de conectividad de red.
- El servidor Avamar tiene un problema de hardware.

Las credenciales no coinciden
Para resolver un error de coincidencia de contraseña, haga clic en el mensaje de advertencia en el panel **Backup server** y proporcione la contraseña correcta.

Solución de problemas del monitoreo de estado

Si hay un problema con SNMP o uno de los procesos de monitoreo de estado, la pestaña **Health** no puede mostrar datos.

Errores de validación de SNMP
De forma predeterminada, ACM valida la configuración de SNMP del switch y los servidores de Dell cada 4 horas. Si ACM detecta que la configuración de SNMP para un componente está desactivada o ausente, corrige automáticamente la configuración.

Si ACM no puede conectarse con uno de los componentes en su IP interna, se muestra el siguiente mensaje en la pestaña **Health**: `Failed to validate SNMP configuration on component(s) <unreachable-component>`

Para resolver este problema:

1. Verifique que las direcciones IP internas del servidor DP4400 sean accesibles en la red.
2. Si el componente es accesible en la red, verifique la conectividad del protocolo SSH al intentar conectarse con la contraseña predeterminada del protocolo SSH. Si no se puede establecer una conexión de protocolo SSH, revierta la contraseña del protocolo SSH en el componente a la contraseña predeterminada.

Nota

Consulte Cambio de contraseñas y sincronización de componentes para saber cómo cambiar las contraseñas y sincronizar los componentes.

Errores de los procesos del monitor de estado
Si el puerto del receptor de SNMP, el servicio de Message Broker o el servicio de base de datos están inactivos, se muestra el siguiente mensaje en la pestaña **Health**: `Health monitor processes are down : <process>`

Para resolver este problema, conéctese a ACM mediante el protocolo SSH y siga el procedimiento que corresponda al mensaje de error:

- Si el puerto del receptor de SNMP está inactivo, verifique que esté activado el puerto 161. Si el puerto está activado y el problema continúa, reinicie el servicio Tomcat con el siguiente comando:

  ```
  service dataprotection_webapp restart
  ```

- Si el servicio de Message Broker está inactivo, verifique que el servicio RabbitMQ esté en ejecución con el siguiente comando:

  ```
  service rabbitmq-server status
  ```

  Si el servicio no está en ejecución, inícielo con el siguiente comando:

  ```
  service rabbitmq-server start
  ```

- Si el servicio de base de datos está inactivo, verifique que el servicio PostgreSQL esté en ejecución con el siguiente comando:

  ```
  service dataprotection_database status
  ```

  Si el servicio no está en ejecución, inícielo con el siguiente comando:

  ```
  service dataprotection_database start
  ```

CAPÍTULO 5

Recursos adicionales

En este capítulo, se proporcionan referencias a otros materiales relacionados con IDPA y los componentes individuales.

Se abordarán los siguientes temas:

Referencias de documentos para IDPA

El conjunto de documentación IDPA incluye las siguientes publicaciones:

- *Integrated Data Protection ApplianceDP4400 Guía de instalación*
  Instrucciones para instalar el hardware de IDPADP4400.
- *Integrated Data Protection ApplianceDP4400 Guía de introducción*
  Explica cómo realizar las tareas iniciales de configuración de IDPA y cómo comenzar con funcionalidad básica, como respaldo y restauración.
- *Integrated Data Protection Appliance Guía del producto*
  Proporciona la información de descripción general y administración del sistema IDPA.
- *Integrated Data Protection Appliance Notas de la versión*
  Información de producto sobre la versión actual de IDPA.
- *Integrated Data Protection ApplianceDP4400 Guía de procedimiento de servicio*
  Los procedimientos para reemplazar o actualizar los componentes de hardware de IDPA.
- *Integrated Data Protection Appliance Guía de configuración de seguridad*
  Información sobre las funciones de seguridad que se usan para controlar el acceso de red y de los usuarios, monitorear el acceso al sistema y su uso, y permitir la transmisión de datos de almacenamiento.
- *Integrated Data Protection Appliance Guía de compatibilidad de software*
  Información sobre los componentes de software y las versiones que se usan en el producto IDPA.

Referencias de documentos para los componentes individuales

Se puede obtener la documentación para estos componentes de Soporte en línea en https://support.emc.com.

Nodo de almacenamiento con protección
El siguiente documento contiene información que se relaciona con Data Domain:

- *Data Domain Operating System: guía de administración*
  En esta publicación, se explica cómo administrar sistemas Data Domain con un énfasis en los procedimientos que usan Data Domain System Manager.

Nodo de servidor de respaldo
Los siguientes documentos contienen información que se relaciona con Avamar:

- *Avamar Guía de administración*
  En esta publicación, se describe cómo configurar, administrar, monitorear y mantener un servidor Avamar.
- *Avamar y Guía de integración de sistemas Data Domain*
  En esta guía, se incluyen procedimientos para configurar el servidor Avamar para ejecutar las operaciones de nivel de nube en el sistema Data Domain.
- *Avamar para VMware: guía del usuario*
  En esta publicación, se describen diferentes métodos y estrategias para proteger las máquinas virtuales de VMware.
- *Avamar Guía del usuario de NDMP Accelerator para Oracle ZFS*

En esta publicación, se describe cómo instalar, configurar, administrar y usar Avamar NDMP Accelerator (acelerador) para respaldar y restaurar los dispositivos de almacenamiento Oracle ZFS admitidos.

- *Avamar Guía del usuario de NDMP Accelerator para filers de NetApp*
  En esta publicación, se describe cómo instalar, configurar, administrar y usar Avamar NDMP Accelerator (acelerador) para respaldar y restaurar los filers de NetApp admitidos.
- *Avamar Guía del usuario de NDMP Accelerator para sistemas NAS de EMC*
  En esta publicación, se describe cómo instalar, configurar, administrar y usar Avamar NDMP Accelerator (acelerador) para respaldar y restaurar los sistemas EMC Isilon, Unity, VNX, VNXe y Celerra admitidos.
- *Avamar para VMware: guía del usuario*
  En esta publicación, se describen diferentes métodos y estrategias para proteger las máquinas virtuales de VMware.

Nodo IDPA System Manager

Los siguientes documentos contienen información que se relaciona con Integrated Data Protection Appliance System Manager:

- *IDPA System Manager Notas de la versión*
  Contiene la información más actualizada sobre la versión actual.
- *IDPA System Manager Guía de introducción*
  En este documento, se incluye información sobre cómo implementar Integrated Data Protection Appliance System Manager y, a continuación, comenzar a usar la administración de Integrated Data Protection Appliance System Manager.
- *IDPA System Manager Guía de administración*
  En este documento, se incluye información sobre cómo administrar Integrated Data Protection Appliance System Manager.
- *IDPA System Manager Guía de configuración de seguridad*
  En este documento, se incluye información sobre las características de seguridad y las funcionalidades de Integrated Data Protection Appliance System Manager.

Nodo de creación de informes y analítica

Los siguientes documentos contienen información que se relaciona con Data Protection Advisor:

- *Data Protection Advisor Guía de instalación y administración*
  En esta publicación, se describe cómo instalar, mantener y configurar DP Advisor.
- *Data Protection Advisor Guía del producto*
  En este documento, se brinda información sobre cómo usar la consola web de DP Advisor para ejecutar y crear informes, visualizar alertas y ver el estado de las operaciones de replicación.

Búsqueda de almacenamiento

El siguiente documento contiene información que se relaciona con Data Protection Search:

- *Guía de instalación y administración de Data Protection Search*
  En esta publicación, se describe cómo instalar, mantener y configurar Search.

Recuperación ante desastres en la nube

Los siguientes documentos contienen información que se relaciona con DD Cloud DR y CDRA:

- *Notas de la versión de Data Domain Cloud Disaster Recovery*

Contiene información complementaria sobre DD Cloud DR y la información más actualizada sobre la versión actual.

- *Guía de instalación y administración de Data Domain Cloud Disaster Recovery*
  En este documento, se describe cómo instalar, implementar y utilizar el producto de DD Cloud DR.

Recursos de capacitación de IDPA

Hay videos paso a paso, demostraciones y explicaciones de características del producto disponibles en línea.

Puede obtener más información y capacitación de IDPA en https://education.emc.com, por ejemplo:

- Descripción general de Integrated Data Protection Appliance 2.2 DP4400
- Introducción a Integrated Data Protection Appliance 2.2 DP4400
- Mantenimiento de CRU de Integrated Data Protection Appliance 2.2 DP4400
- Descripción general de Integrated Data Protection Appliance 2.2 System Manager
- Monitoreo de alertas de Integrated Data Protection Appliance 2.2